

MALWARE ANALYSIS OF ZEUS BOTNET

Malware Analysis Project

MSc in Cybersecurity

Oluwaseun Odunibosi

Student ID: 18123970

School of Computing

National College of Ireland

Lecturer: Moldovan

MALWARE ANALYSIS OF ZEUS BOTNET

Oluwaseun Odunibosi

STUDENT ID: 18123970

Table of Contents

[1.0 EXECUTIVE](#_Toc532113552) SUMMARY………………………………………………………………………………….2

[2.0 METHODOLGY](#_Toc532113554)……………………………………………………………………………………………..3

[2.1 VIRTUAL](#_Toc532113555) LAB SETUP……………………………………………………………………………………..3

[2.2 BOT](#_Toc532113556)/VICTIM MACHINE SETUP……………………………………………………………………..3

[2.3 ZEUS](#_Toc532113557) C&C SERVER SETUP……………………………………………………………………………..3

[2.4 SOFTWARE](#_Toc532113558) AND ONLINE TOOLS DESCRITPTION…………………………………………..4

[2.5 ZEUS](#_Toc532113559) VARIANT PCAP…………………………………………………………………………………….4

[3.0 IDENTIFICATION](#_Toc532113561) OF ZEUS BOTNET……………………………………………………………….5

[3.1 BOTNET](#_Toc532113562) SIZE AND DAMAGE…………………………………………………………………………5

[3.2 TARGET DEVICE](#_Toc532113563)……………………………………………………………………………………………5

[3.3 BOTNET](#_Toc532113564) ARCHITECTURE……………………………………………………………………………..6

[3.4 BOTNET](#_Toc532113565) BEHAVIUOR………………………………………………………………………………….7

[3.5 BOTNET ARCHITECTURE](#_Toc532113566)…………………………………………………………………………….7

3.6 BOTNET RESILLENCE…………………………………………………………………………………..7

[3.7 BOTNET](#_Toc532113569) TAKEDOWN………………………………………………………………………………….7

3.8 BOTNET EVOLUTION…………………………………………………………….8

4.0 RECOMMENDATION………………………………………………………………9

5.0 CONCLUSION…………………………………………………………………….9

6.0 REFERENCES…………………………………………………………………….10

7.0 APPENDIX………………………………………………………………………….11

# Executive Summary

The threat of botnet in recent decades has been on the rise, the name Botnet was culled from the words “robot” and “networks”. A botnet can the defined as the connection of infected computers which are remotely controlled and commanded by an attacker called botmaster to perform malicious activities, usually infected computers will join a network of other infected computers and await command from the threat actor in control. Botnet can be use to perform many malicious activities like tracking and stealing of user credentials, personal information and even use to initiate fraudulent banking transaction on behalf of victims online, an example is the Zeus botnet (Zbot) used to steal users online banking credentials and execute fraudulent transactions on behalf of the victim. The Zeus botnet will be analyzed in this report.

The Zeus botnet (Zbot) is a Trojan horse malware kit operating on several Microsoft windows. It uses keylogging and http form grabbing techniques to steal financial information of victim. Zeus was first detected or identified in the year 2007 when it was used to steal information from the transport department of United States. The level of attack of Zeus and its variants ranges from users whose banking details was compromised, large public and companies. There are so many variant of Zeus in the wild with more resilient power than Zeus itself with techniques like Domain Generation Algortihm DGA and FastFlux been used to make it difficult to shutdown.

In 2012, Micorosft took action to takedown the GameOver Zeus variant but it had no effect because of the network architecture of the botnet and in the year 2014, the department of Justice work jointly with other agencies in an operation called Tovar to break communication between the GameOver Zeus bots and the C&C servers and was successful, subsequently the FBI announced a reward estimated at USD 3 million for anyone who has information about the Cybercriminal named Evgeniy Bogachev from Russia linked with GameOver Zeus.

The report will also detail the lab setup and tools used in the analysis of the Zeus variant and also talk about the behaviour of the Zeus variant.

Lastly, the report will recommend how individual, organisation and can protect themselves against this attack like Denying all connections that are inbound and allow only trusted services by using firewall, also make sure you apply strict password policy; which makes it hard for attackers to crack password files even on compromised systems.

# Methodology

This report will look at the different approaches through which the Zeus botnet can be detection and countermeasures. The approach we will be using is below

**Internet Search Static Analysis Dynamic Analysis Result**

**2.1 VIRTUAL LAB SETUP**

Two components will be use in our virtual lab setup but before installing any tools on these virtual machine; we must isolate the virtual machines from the physical host by assigning bridged connection within the network to the virtual machines. This is done so that our virtual machine will give the same DHCP and DNS with different MAC. Note that the bridged network showing connection to the outside world is not really connected to the outside world but rather it is bridged internally between our two virtual machine i.e. it only act as a pass through and Zeus malware cannot infiltrate our host network. Fig 1 in appendix shows the lab setup

**2.2 BOT/VICTIM MACHINE SETUP**

Our Victim machine will be running on window 7 OS, this machine is also where our bot will be generated and executed. The config.txt file will be setup in a way that enables access of bot to C&C on the IP address assigned to it. There are three things needed to build this bot executables and are: a builder which will be use to create configuration file that are encrypted and bot executable suitable to each victim, Configuration file which will contain address where information stolen will be sent, it will also contain URL where file will be located. The third is the web injects, which will contain file for injecting HTML into websites that are targeted to gather sensitive information. By using the configuration file binary generated by bot configuration builder; bot executables are generation then executed and the zeus configuration installation tab is used to verify this

The second phase of setting up the victim machine is to install all tools for bot analysis. Wirehark will be installed to captures network traffic packets generated by bot victim machine to communicate with C&C server is installed. Procmon which is will be use to observe the execution and building behaviour and the PE Explorer tool which will be use for reverse engineering will be installed. Intrusion Detection System tool Snort will also be installed on the bot victim machine.

**2.3 THE ZEUS C&C SERVER SETUP**

The Command and control server of Zeus will involve installing a Zeus toolkit which contains PHP scripts that helps botnet owner to monitor status of their bots, helps issues command and recover information collected. XAMP server will be installed to carry out this process on our second virtual machine. Integration of XAMP with Zeus toolkit follows immediately and this involves using bot PHP script to setup required database tables, user specific data and this will be base on the configuration file use to generate the bot. Copy all files in the “Server[php]” folder inside the Zeus files into htdocs folder in XAMPP. The next step is to create a database for command and control with necessary requirement. Wireshark is also installed on the server to monitor inbound and outbound network traffic generated by control panel. Once complete, our command and control Server can be use to control bots which will be sent to victim machine.

**2.4 SOFTWARE AND ONLINE TOOLS DESCRIPTION**

**HYPERVISORS:**

**VMWARE PRO:** Known for its high performance and comes with extra features like desktop virtualization, virtual machine sharing that makes it useful for complex virtual network. VMware will be for our report.

**VIRTUAL BOX:** It also offers wide range of features for virtualization though doesn’t offer same level of support in term of 3D graphics which can be an issue for heavy users. It doesn’t also exchange disk images with some other hypervisor except VMware.

**SERVERS:**

**XAMPP SERVER:** this is a cross platform open sour web server which consists of Apache, HTTP server, MariaDB database, MySql database, PHP and PERL programming language. It is lightweight making it easy to for developers to create local web server which can be use for testing and development purpose. This will be use in our report.

**WAMP SERVER:** The WAMP servers only run on window platform and support only Apache, MySql, PHP server.

**PROCESS MONITORING TOOLS**

**PE EXPLORER:** Is a reverse engineering tools which is use for investigating executable files like EXE, DLL, SYS, SCR, it can also be use for extensive binary security analysis and auditing of binary processes, it also have the ability to edit, view element of an executable file, it is widely use, and also been tested and will be use in our report.

**PE STUDIO:** A tool use to detect anomaly in executable files, it also gives information about the programming language use to code the program.

**NETWORK MONTORING TOOLS**

**WIRESHARK:** Is a tool use for capturing packet data in the course of network analysis, Wireshark captures packet data and display the captured packet data as detailed as possible. It is tested and widely use tool and will be used for our analysis.

**TCPVIEW:** this gives basic information about TCP and UDP connection and also gives details on local and remote address and state of TCP connection.

**INTRUSION DETECTION TOOLS**

**SNORT:** is an open source IDP/ IPS tool which will be used for signature inspection, anomaly detection and protocol based detection. Snort can also be use as packet sniffer and packet logger. It will be use in our analysis.

**OSSEC:** Open source security only run on UNIX like system but provide an agent to protect window host when system detect an anomaly or pattern, an alert is displayed on the console and notification is sent by mail.

**2.5 ZEUS VARIANT PCAP**

An analysis found on the site of Malware Capture Facility Project (MCFP DATASET) carried out on ZBOT.OOWO by (Sebastian Garcia in 2014) will be analyzed in this report. The capture was done between the 5th of September and 1st of October 2013, a binary with MD5 value 46b3df3eaf1312f80788abd43343a9d2 was used in the report. Searching through Virus total shows it was classified as Trojan-spy.Win32.Zbot.oowo but the name is not known for sure.

**3. IDENTIFICATION OF ZEUS BOTNET**

This report will detail information about the Zeus bot sample, type of file, its name, size, hashes and current anti virus detection capabilities. We will check result from Virus Total to perform a quick analysis of our sample.

Result from Virus Total gives the following basic properties

**MD5** 2464355c63e0e31c9f013b79becc0a85

**SHA-1** 925a116b78c88b240b0a75b5afeefaf36162d5

**Authentihash** eOb198c7dff4427894f4547e1ad4cb3a531413cad8eb9a27588d47ddfd8016e8

**IMPHASH** 09856ea049ee0244c3e890c703547110

**FILE TYPE** Win32 EXE

**MAGIC** PE32 executable for MS Windows (GUI) Intel 80386 32-bit

**SSDeep** 6144:eT+FQogd7PswMHSclOq1G/PJRnC2CkErfoe:RFhgkycBqwJRC2gce

**TRiD** Win32 Dynamic Link Library (generic) (38.3%)

Win32 Executable (generic) (26.2%)

OS/2 Executable (generic) (11.8%)

Generic Win/DOS Executable (11.6%)

DOS Executable Generic (11.6%)

**File Size** 321.66 KB

The Virus total result also shows that 61 out of 69 antivirus developers detected the file as been malicious and dangerous with some noticeable antivirus company like AVG detecting it as Win32:Jorik-NH [Trj], McAfee as PWS-Zbot.gen.alg, Malwarebytes as Trojan.Zbot and Comodo detected it as [TrojWare.Win32.Agent.KDFK@4qfvey](mailto:TrojWare.Win32.Agent.KDFK@4qfvey), this shows a poor antivirus coverage. It also shows the Portable Executable info and functionalities imported from the external dynamic link libraries as shown in Fig. 2,3,4 in the appendix. Virus total also shows the behavioral analysis of the gameover zeus sample, it gives detail of the following;

* When the file been studied was executed, some network communication were been observed like UDP communication with IP address like 99,.75.9.186: 28981
* It also shows information about what the sample does to the registry of the file system of the sandbox environment like files opened, files read, written and deleted

**\Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option**

* It also perform some process and service action the sandbox environment like creating of process, shell commands, process injection and process termination.
* It also created and opened a mutexes for signals and synchronization.
* Load modules and use of the following dynamic functionalities like rcpcrt4.dll, advapi32.dll, netapi32.dll etc

**3.1 BOTNET SIZE AND DAMAGE**

One of the most common way to measure the size of a zeus botnet is the description of that botnet in terms if size( in terms of number of host that are compromised. This serves as a factor for various zeus effect and damages. The two aspect that can be use to distinguish a zeus botnet size are

* A botnet footprint which is the total number of machine that are compromised with a certain specimen of Zeus which are commanded and controlled at any point in time.
* The live population of the Zeus botnet which is the current number of hosts which interacts with C&C server at specific point in time.

Abuse.ch which is a tracking service created a Zeus crimeware toolkit for tracking Zeus. From the report, 144 online servers were used to monitor Zeus online server.

The Zeus malware recorded high number of variants with one noticeable variant called gameover Zeus in 2009. It was approximated to have caused damage of around US$100 million since it was first detected according to a whitepaper report by UNISYS although figures may be higher now since no government agency or bodies tracks report on amount lost and victim organisation.

The spread of Zeus have caused financial damage to so many companies around the world with the Zeus accounting for 44% of all banking infections according to a security company Trusteer. Smile Zone, a dental company lost about $205,000 in March 2010 after being affected by a Zeus variant. ESkola LLC, a Tennessee based company in United States in the medical filed lost $130,000 and $46,000 respectively when it was attacked by a Zeus variant.

The Spread of Zeus and its variants have also caused damage of goodwill with flurry of victims of online fraud heading to court to recover some of the money lost from their bank.

It is difficult to exactly trace the number of systems affected by Zeus since inception it has been estimated that the United State alone has the largest chunk. As at April 2010, research indicated that almost 88% of fortune 500 companies were infected with the malware. Zeus targets top level international domains belonging to large multinationals. The top five countries affected by Zeus in terms of machines are Egypt with 19%, Mexico with 15%, Saudi Arabia with 13%, Turkey with 12% and United State with 11% according to UNISYS report in (2010). The Fig 5 in the appendix shows the top domains that are targeted by Zues.

**3.2 TARGET DEVICES**

The Zeus has been known to attack mobile phones platforms and PC running windows. Recently, online banking services security features are TAN codes (Transaction Authentication Number) with digital signatures. Zeus trojan for mobile platform (Zitmo) was first detected in 2010 and became the first maliciously designed program to steal mTAN codes. Zitmo intercepts passwords sent to user phone during two factor authentication thereby creating fraudulent money transfers and also verifying them.

Zeus running on PC has also been available for a long time; when a user whose computer have been infected attempt to log in to his/her bank webpage, Zeus register victim as an address of interest, it modifies the browser webpage so that user personal information is not sent to bank but to Zeus botnet command centre.

**3.3 BOTNET ARCHITECTURE**

Zeus appears in various forms on the web thanks to variants created by its developers. A new variant of Zeus was discovered by researchers which do not rely on command and control servers (C&C) to receive commands.

The Zeus variant uses peer-to-peer communication for transferring command from hosts that are compromised and belonging to a botnet infrastructure. This new variant is use as backup in case the C&C servers are off the map or unreachable. Each node will operate as master or slave and gives orders to the other bots. Each bot can work as a client which can carry out orders as a command server due to presence of a light web server like nGix which equip the malware, communication between nodes are based on HTTP protocol.

From the pictures below; tracking of p2p botnet requires complete enumeration of node while the earlier version only finds the Command and Communication server. A technique commonly use in the enumeration of compromised host is called recursive crawling, Passive Monitor (PPM) which enumerate host that are infected regardless of whether they are behind firewall or NAT can also be used.

To avoid dumping of traffic and tracking, botnet authors uses UDP protocols for communication instead of TCP protocols that can be detected easily. Handshake phase between bots is made possible by homemade UDP and after successful connection, exchange of TCP data like config files, list of other peers etc are started.

Supervisor bot will send command to infected zombie peer who then transfer it to other peers, all acting as zombie army soldier and supervisor bot. It has many controller for hiding and from been seized and shutdown.

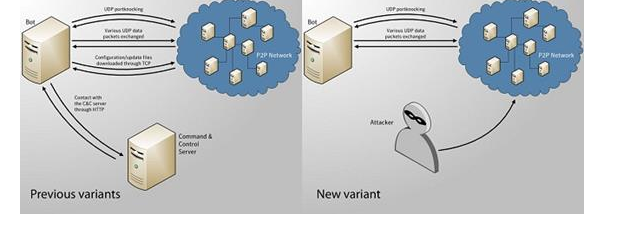


FIG 6: (SOURCE: <https://resources.infosecinstitute.com/botnets-how-do-they-work-architectures-and-case-studies-part-2/>)

**3.4 BOTNET BAHAVIOUR**

Zeus Trojan is developed to steal private information from compromised systems . Zeus Trojan mostly target system information, banking details and online information of victims, this information can be customised using the Zeus toolkit and this can be done by fitting compiled files that are configured into the Trojan installer, this information can later be updated by attacker if so wishes to target other information.

Trojan gathers information like internet Explorer, FTP, POP3 passwords contained within Protected Storage (PStore) upon execution, though the most useful technique for information gathering is by monitoring website that are appear in the configuration file because most times, bot intercept legitimate web pages and insert extra fields .

The Zeus can also contact Command and Control servers to make available itself to perform additional functions which allow an attacker connected remotely to control Trojan to execute and move files,deleting system files and shutting down system which makes computer not usable until it is reinstalled. The following below is noticed once bot is executed

1. Bot copies itself to %system32%\sdra64.exe

2. Increase its privileges by searching for winlogon.exe and injecting a code and string table to the process thereby creating a thread to code execution and main executable bot stops.

3. Additional code is injected into svchost.exe through code injected in winlogon.

4. A folder named %System%\lowsec with two files local.ds and user.ds inside is created. The user.ds contains the credentials that are stolen and the local.ds contain dynamic configuration.

5. The code injected into svhost is then used for network communication and processes by third party which can be used to steal financial information.

6. Mutexes and pipes are use for the communication between injected components.

FIG.6-10 shows the behaviours of the zeus step by step.

**3.5 BOTNET RESILLIENCE**

Although some variant of Zeus have been brought down, newer versions that uses some resilience techniques like DGAs and Fastflux have been detected.

The earlier version of Zeus uses a p2p to maintain contact, accept command and perform instructions from C&C servers but the recent variant of Zeus like gameover zeus uses a randomized (DGA) domain generation algorithm which is released about few minutes after infection of a PC, domain names which looks random are calculated based on the date and malware reaches out through to the internet to see if that domain exists and if it does, calls home to the conect C& C server. If any C&C servers get blocked, shutdown or domain is discovered and blocked, Malware developer can register another domain from list of domain that has been generated in advance and resume communication, this makes the malware very difficult to detect and block.

Another resilience factor is the communication protocols used by new variant of Zeus; the new variant of Zeus uses fastflux which allows an attacker to program malware to create few domain names in a day and swap the IP address which is associated with these domain names quickly enabling them to avoid blacklisted IP. It also helps rechannel C&C communications to hide behind many proxy servers to hide their activities.

**3.6 BOTNET TAKEDOWN**

The Justice department and Federal Bureau of Investigation (FBI) of United States announced an international joint effort with private industry in the effort to bring down the GameOver zeus botnet in the year 2014. The operation was tagged “Operation Tovar”. FBI launched the operation by introducing its own peers inside the botnet; this was done in order to return the p2p network back to a centralized one. Internet service providers (ISP) were also asked to provide investigators power over proxy nodes used by attackers in order to connect the C&C to the botnet; this was done to prevent the operators of Gameover Zues from mitigating the attack from C&C botnet machines. Bots started connecting to the proxies used and controlled by FBI and this effectively takedown the GameOver Zeus.

Prize money of $3 million was put on the owner of Zeus head (Bogachev) after the successful takedown.

**3.7 BOTNET EVOLUTION**

The Zeus botnet (Zbot) is a Trojan horse malware kit operating on several Microsoft windows. It uses keylogging and HTTP form grabbing techniques to steal financial information of victim. Zeus was first detected or identified in the year 2007 when it was used to steal information from the transport department of United States. The level of attack of Zeus and its variants ranges from users whose banking details was compromised, large public and companies. There are so many variant of Zeus in the wild with more resilient power than Zeus itself with techniques like Domain Generation Algortihm DGA and FastFlux been used to make it difficult to shutdown. Some variant of the Zeus botnet are below

* **GameOver Zeus:** A variant of Zeus which rely on the peer to peer botnet infrastructure of the earlier Zeus version but the centralized command and control server was removed and a DGA (domain generation algorithm) which produces new domains was added in case peer is not reachable, all peers in the botnet also act independently as command control (C&C) servers. It is estimated to have infected more than 1 million users around the world since first detected.
* **SpyEye Zeus:** This contains a keylogger that retrieves login credential of online bank account and is a toolkit very popular with cybercriminals.
* **Ice IX Zeus:** This is a modified variant of Zeus, is added new features by evading tracker sites which is used in monitoring Command and Control (C&C) servers controlled by Zeus. It is use to steal personal and financial information like password online.
* **Carberp Zeus:** Gives attacker doors to steal online banking information of users from infected system. It is widely used in Russia.

**4 RECOMMENDATION**

For organisation and individual to protect themselves against the Zeus botnets and its variants, it is recommended that

1. Deny all incoming connections and allow only services you want to offer the outside world by using firewall.
2. Make sure you apply strict password policy; this makes it hard for attackers to crack password files even on compromised systems.
3. Disable autoplay so as to prevent automatic launching of executable files on network and removable drives.
4. Train staffs and users not to attachment from mails or any other means unless they are expecting them.
5. Configuration of mail server to block emails which contains attachments that are used in spreading the malicious malware.
6. Isolation of infected computers immediately to prevent further spreading of malware.
7. Installation of malware detecting antivirus on all system and constant updating.

Organisations can also configure Intrusion Detection System that detect anomaly or change in pattern of network or host system and raise an alert using certain rules.

**5 CONCLUSION**

Since the detection of Zeus in 2007, concerted effort has been made by government and private bodies round the world to shutdown it operation; though quiet successful but the development of more resilience variant of Zeus botnet that using techniques as Domain generation Algortihm and Fastflux to hide themselves in recent year, it has been very challenging and more effort will be needed to shutdown this botnets. As recommended in this report; users and organization should be on the lookout so they don’t fall victim.

**6. REFERENCES**

1. Andra Zaharia, 2016. The Top 10 Most Dangerous Malware That Can Empty Your Bank Account [Updated]. Heimdal Security Blog. URL <https://heimdalsecurity.com/blog/top-financial-malware/> (accessed 4.27.19).

2. Category: P2P [WWW Document], n.d. . Malware Capture  facility project. URL <http://mcfp.weebly.com/1/category/p2p> (accessed 4.27.19).

3. Dieterle, A., 2010. Zeus Botnet TCP/IP Packet Capture in Netwitness Investigator. CYBER ARMS - Computer Security. URL <https://cyberarms.wordpress.com/2010/04/15/zeus-botnet-tcpip-packet-capture-in-netwitness-investigator/> (accessed 4.25.19).

4. Documents and Resources from the Gameover Zeus / Cryptolocker Press Conference [WWW Document], 2014. URL <https://www.justice.gov/archives/opa/documents-and-resources-gameover-zeus-cryptolocker-press-conference> (accessed 4.26.19).

5. Franceschi-Bicchierai, L., 2015. How the FBI Took Down the Botnet Designed to Be ‘Impossible’ to Take Down. Motherboard. URL <https://motherboard.vice.com/en_us/article/539xy5/how-the-fbi-took-down-the-botnet-designed-to-be-impossible-to-take-down> (accessed 4.27.19).

6. Guerrino\_Decl\_Ex1.pdf, n.d.

7. International Law Enforcement Sinkhole GameOver Zeus and CryptoLocker Botnets [WWW Document], 2014. . Infosecurity Magazine. URL <https://www.infosecurity-magazine.com:443/news/international-law-enforcement-sinkhole-gameover/> (accessed 4.26.19).

8. MAthew J. Schwartz, 2014. Gameover Zeus Trojan Returns [WWW Document]. Gameover Zeus Trojan Returns. URL <https://www.bankinfosecurity.com/gameover-zeus-trojan-returns-a-7050> (accessed 4.26.19).

9. Pierluigi Paganini, 2013. Botnets, how do they work? Architectures and case studies – Part 2 [WWW Document]. Infosec Resources. URL <https://resources.infosecinstitute.com/botnets-how-do-they-work-architectures-and-case-studies-part-2/> (accessed 4.26.19).

10. Symantec Security Response, n.d. International Takedown Wounds Gameover Zeus Cybercrime Network [WWW Document]. Symantec Security Response. URL <http://www.symantec.com/connect/blogs/international-takedown-wounds-gameover-zeus-cybercrime-network> (accessed 4.24.19).

11. The inside story on botnets, n.d. 32.

Trojan.Zbot | Symantec [WWW Document], n.d. URL <https://www.symantec.com/security-center/writeup/2010-011016-3514-99> (accessed 4.27.19).

12. U.S. Leads Multi-National Action Against GameOver Zeus Botnet and Cryptolocker Ransomware, Charges Botnet Administrator [WWW Document], n.d. . Federal Bureau of Investigation. URL <https://www.fbi.gov/news/pressrel/press-releases/u.s.-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware-charges-botnet-administrator> (accessed 4.26.19).

13. Waheed, S., n.d. IMPLEMENTATION AND EVALUATION OF A BOTNET ANALYSIS AND DETECTION METHODS IN A VIRTUAL ENVIRONMENT 102.

14. ZeuS-in-the-Mobile – Facts and Theories [WWW Document], n.d. URL <https://securelist.com/zeus-in-the-mobile-facts-and-theories/36424/> (accessed 4.26.19).

**7 APPENDIX**

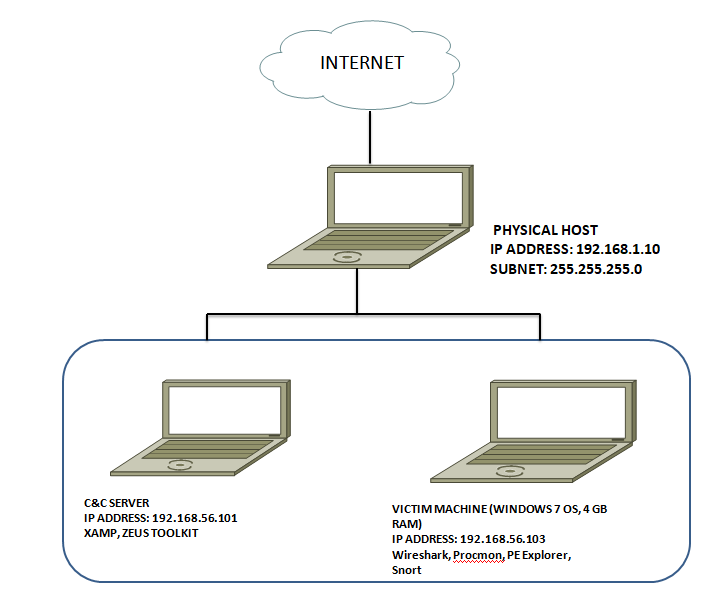


FIG 1: Shows the Lab setup for our test environment with firewall.

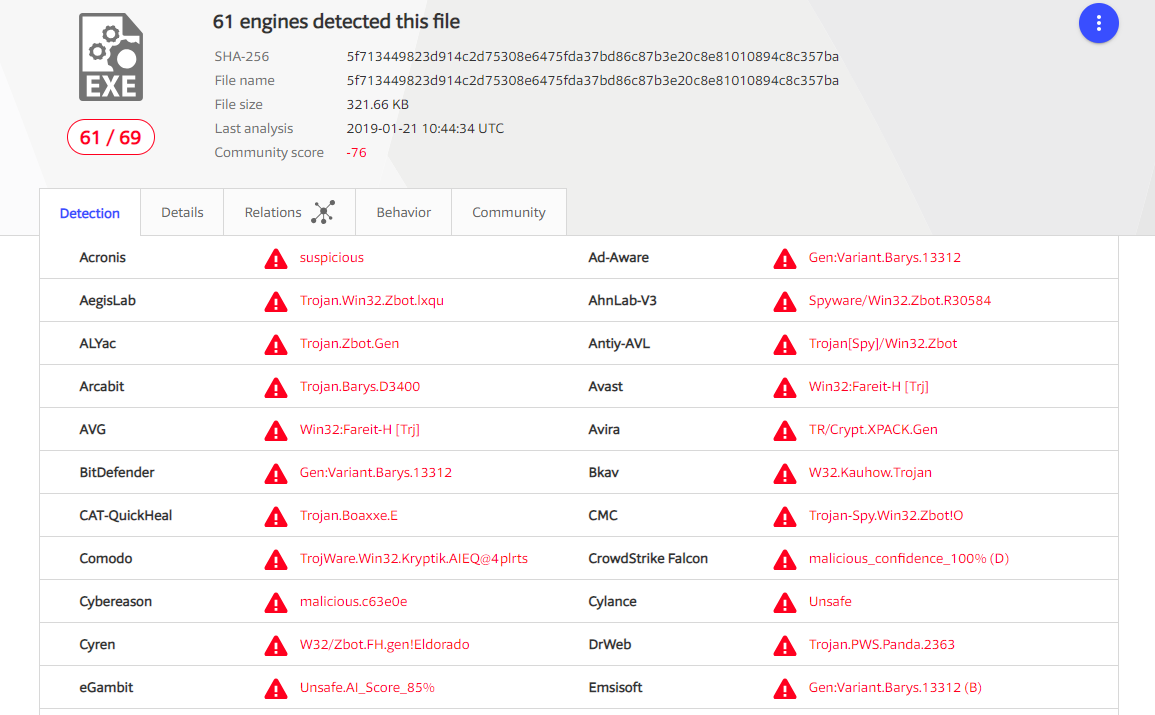


FIG 2: shows the antivirus detection rate by antivirus company

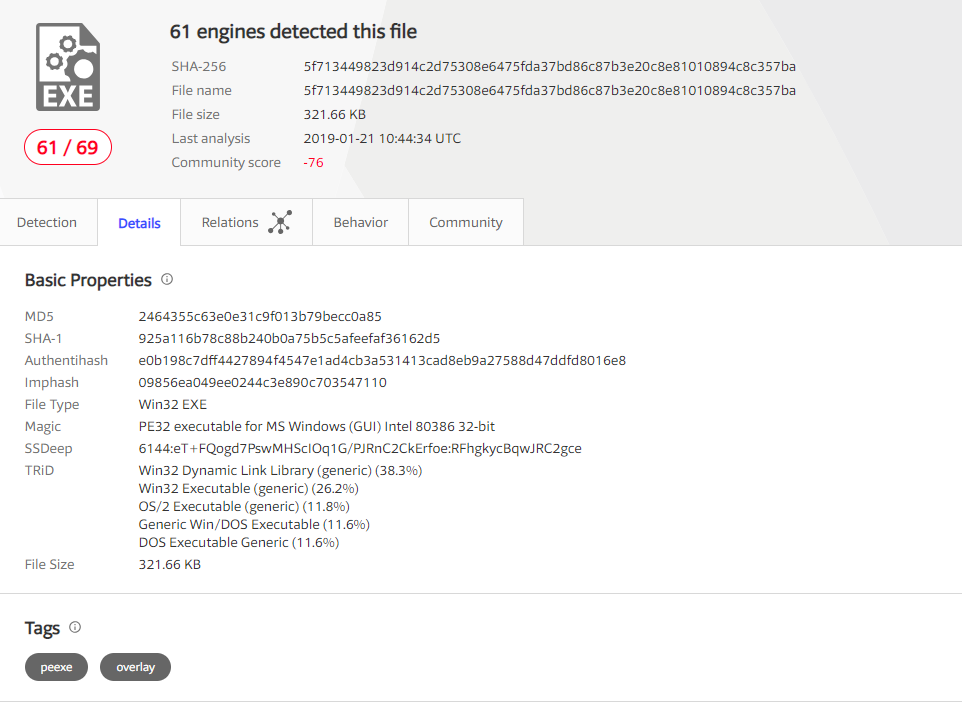


FIG 3: Shows virustotal details which include hash, fitle type and file size

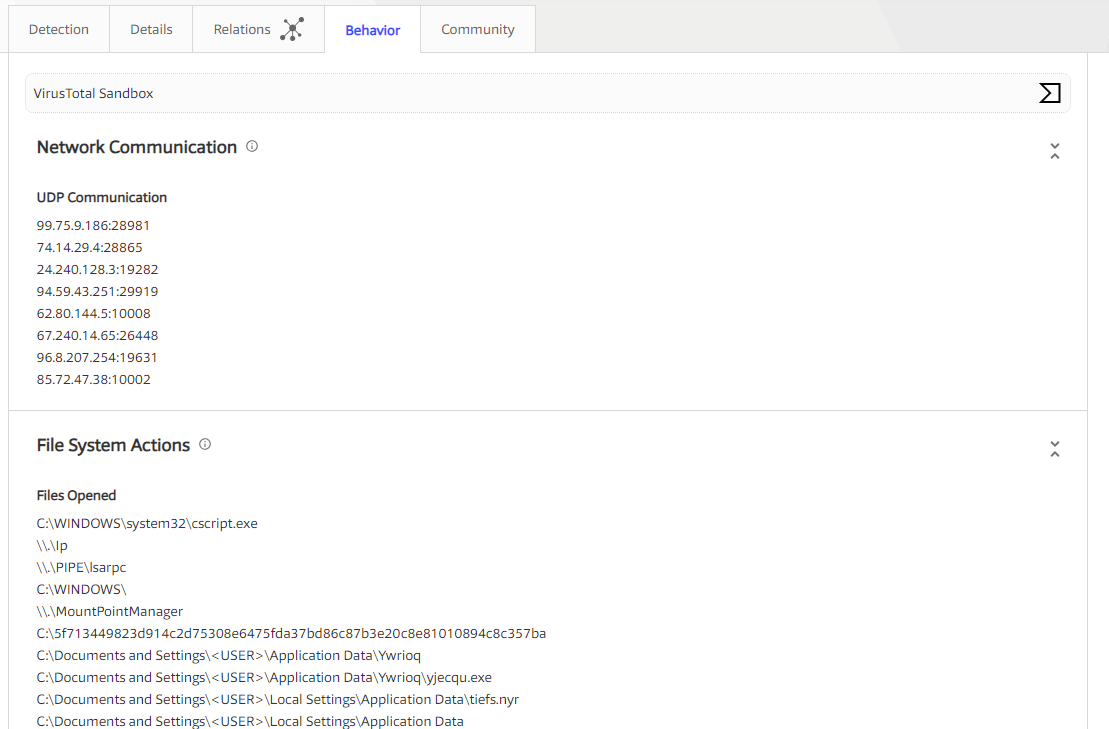


FIG 4: Shows behavioral result from virustotal

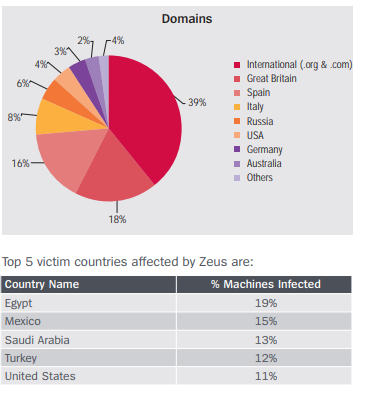


FIG 5: shows the top domain affected by Zeus and the top five countries



FIG 6: A Zeus SPAM impersonating the FDIC

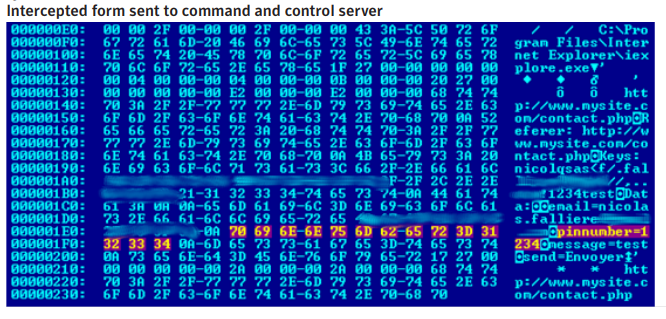


FIG 7: INTERCEPTED FORM SENT TO C&C SERVER

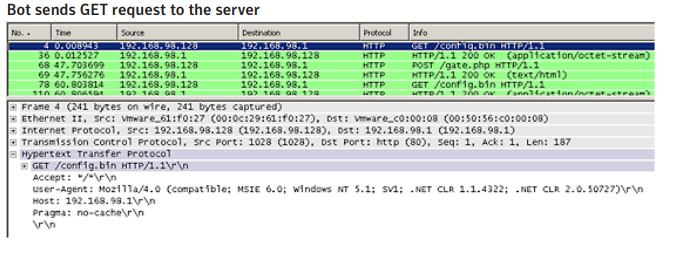


FIG 8 : Network communication using GET request to the server

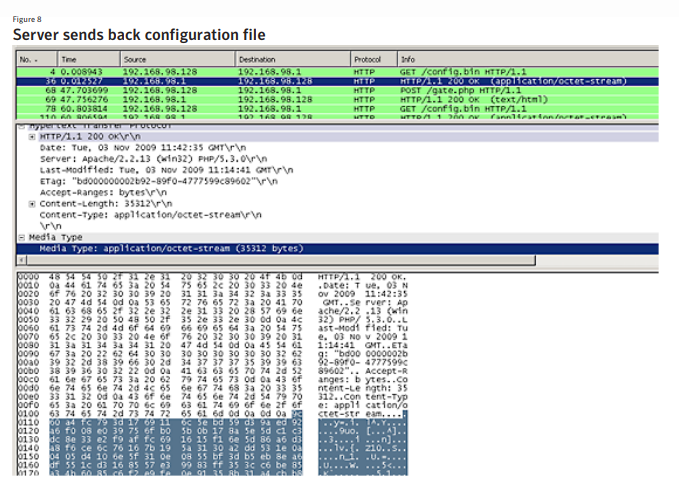


FIG 9: C&C Server reply

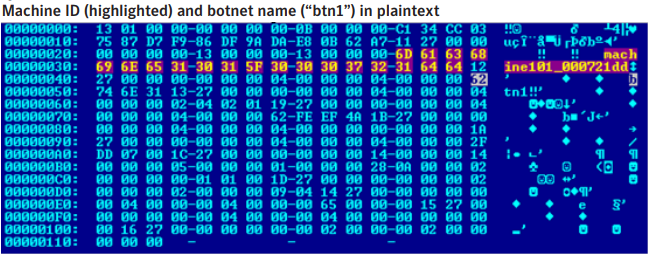


FIG 10: Shows a typical post reply sent after decryption